

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
16 June 2005 (16.06.2005)

PCT

(10) International Publication Number
WO 2005/055020 A1

(51) International Patent Classification⁷: **G06F 1/00**,
H04L 29/06

(21) International Application Number:
PCT/IB2004/003984

(22) International Filing Date: 2 December 2004 (02.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03293035.6 4 December 2003 (04.12.2003) EP

(71) Applicant (for all designated States except US): **AXALTO SA** [FR/FR]; 50 Avenue Jean-Jaures, F-92120 Montrouge (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **PEPIN, Cyrille**

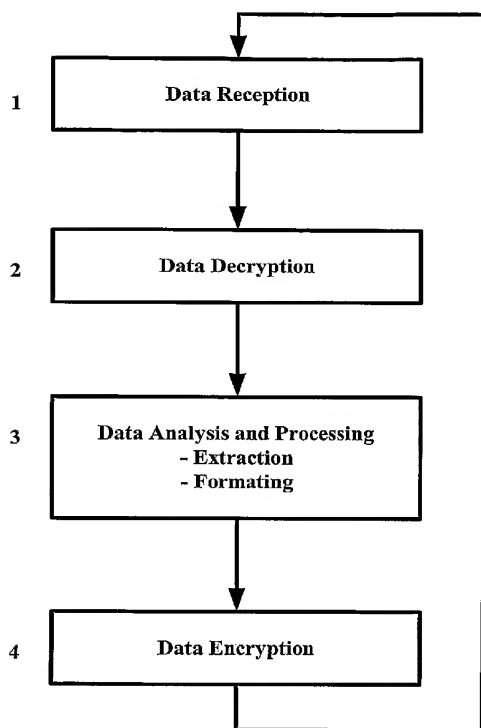
[FR/FR]; c/o Intellectual Property Dpt, 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR). **RAIN-SARD, Stéphane** [FR/FR]; c/o Axalto SA, Intellectual Property Dpt, 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(74) Common Representative: **AXALTO SA; PATRICIA RENAULT**, Intellectual Property Dpt, 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR ENCRYPTION AND DECRYPTION ON THE FLY



(57) Abstract: This invention concerns a method to ensure the security of encrypted data transmitted in blocks to an electronic assembly in several steps. The method consists, when said assembly receives a block, in decrypting the block received, processing the information contained in said block and in encrypting the processed information.

5 Reception of next data

WO 2005/055020 A1



(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*